Zina *et al. EURASIP Journal on Wireless Communications and Networking* (2016) 2016:85
DOI 10.1186/s13638-016-0567-7

EURASIP Journal on Wireless Communications and Networking
a SpringerOpen Journal

RESEARCH Open Access

Location privacy preservation in secure crowdsourcing-based cooperative spectrum sensing

Chkirbene Zina[1,2], Mazen Hasna[1], Ridha Hamila[1*] and Noureddine Hamdi[2]

Abstract

Spectrum sensing is one of the most essential components of cognitive radio since it detects whether the spectrum is available or not. However, spectrum sensing accuracy is often degraded due to path loss, interference, and shadowing. Cooperative spectrum sensing (CSS) is one of the proposed solutions to overcome these challenges. It is a key function for dynamic spectrum access that can increase largely the reliability in cognitive radio networks. In fact, several users cooperate to detect the availability of a wireless channel by exploiting spatial diversity. However, cooperative sensing is also facing some series of security threats. In this paper, we focus on two major problems. The first problem is the localization preservation of the secondary users. In fact, malicious users can exploit spatial diversity to localize a secondary user by linking his location-dependent sensing report to his physical position. The existing solutions present a high level of complexity which decreases the performance of the systems. The second problem is the data injection attack, in which malicious CR users may affect the decisions taken by the cognitive users by providing false information, introducing spectrum sensing data falsification (SSDF). In fact, they can submit false sensing reports containing power measurements much larger (or smaller) than the true value to inflate (or deflate) the final average, in which case the fusion center may falsely determine that the channel is busy (or vacant) which increases the false alarm and miss detection probabilities. In this paper, we propose a novel scheme to overcome these problems: iterative per cluster malicious detection (IPCMD). It utilizes applied cryptographic techniques to allow the fusion center (FC) to securely obtain the aggregated result from various secondary users without learning each individual report. IPCMD combines the aggregated sensing reports with their reputation scores during data fusion. The proposed scheme is based on a new algorithm for key generation which can significantly reduce the key management complexity and consequently increase the system performance. Therefore, it can enable secure cooperative spectrum sensing and improve the secondary user location privacy.

Keywords: Secure cooperative spectrum sensing, False sensing reports, Location privacy, Data injection attack

1 Introduction

Due to the increasing demand on advanced broadband wireless technologies and services added to the wide spread of new operators, the static frequencies and inflexible spectrum management policies became obsolete and resulted in a spectrum scarcity problem. In fact, it has been confirmed by multiple spectrum measurement campaigns that this scarcity is only virtual and is caused by the underutilization of the bandwidth [1, 2]. Thus, more effective spectrum management techniques emerged to effectively exploit the precious radio resources. CR is considered as an intelligent wireless communication system which can exploit these underutilized spectral resources by reusing unused spectrum in an opportunistic manner [3, 4].

Cognitive radio systems involve primary users (PU), the owners of licensed spectrum, and secondary users (SU) who sense the radio environment and intelligently operate the unused spectrum under license and renounce if the primary users are active. Secondary users identify the received signal strength, interference, and the number of

*Correspondence: hamila@qu.edu.qa
[1] Department of Electrical Enginnering, Qatar University, Doha, Qatar
Full list of author information is available at the end of the article

users residing in the spectrum and observe the heterogeneous spectrum that varies in time and space due to the activities of primary user [5]. The availability of heterogeneous spectrum depends on the availability of spectrum holes that fluctuate over time and location. The challenge is the identification and detection of primary user signals in harsh and noisy surrounding environment [6–8].

Thus, spectrum sensing is considered as a key function for dynamic spectrum access which is designed to maximize spectrum efficiency and capacity within congested wireless transmission environments and it is a critical function to avoid interference with primary users [9, 10]. However, detection performance in practice is often compromised with multipath fading, shadowing, and receiver uncertainty issues. To overcome the impact of these issues, cooperative spectrum sensing is proposed as an effective method to improve the detection performance by exploiting spatial diversity [3, 8, 11, 12]. While cooperative gain such as improved detection performance and relaxed sensitivity requirement can be obtained, cooperative sensing is facing some series of security threats [13, 14]. In this paper, we consider two types of threat, location privacy leaking [15] and data injection attack in cooperative sensing. The existing works show that similar to geolocating the individuals via Wi-Fi or Bluetooth signals, the correlation of CR sensing reports and their physical location can be exploited by malicious attackers to geolocate a user and thus compromise the user's location privacy [16]. A potential approach to prevent location privacy leaking is privacy-preserving sensing report aggregation (PPSRA) protocol [15]. In fact, all the users have to negotiate their keys together at the same time to be able to keep the sharing fusion center (FC) secret among all participants; the aggregator cannot obtain the aggregation result unless he can collect all of the participants' reports. However, this solution presents one major drawback: key management complexity especially with a large number of participants.

In [17], the authors propose a low-overhead symmetric cryptographic mechanism that reduces the effects of the malicious users on energy efficiency. However, the symmetric key encryption has a major problem. In fact, users must first establish and share a secret key. Then, the key must be exchanged in a secure way. This process is usually inconvenient and requires significant overhead. In [18], the authors present a new scheme that can calculate a trust value for each secondary user based on a comparison between its sensing report and the reports of its neighborhood. However, the trust value may give wrong results in some realizations of the channels if the neighborhood detected wrong sensing report. In [19], an attacker identification algorithm was proposed. It can detect attackers in cluster-based cognitive radio networks. In [20], the authors propose a principal-agent-based joint spectrum sensing and access framework to thwart the malicious behaviors of intelligent malicious users in cognitive radio networks. In [21], the authors proposed a weighted decision fusion scheme that uses past information. However, these solutions do not take into consideration that the principal agent and the FC can be run by an untrusted service provider.

In [22], the authors present a solution for data injection attack. It uses a few trusted anchor detectors to evaluate the instantaneous trustworthiness of mobile detectors in combination with their reputation scores. However, it requires more resources to work (trusted anchor, GPS). Thus, it was possible for them to illegitimately track the individuals from the sensing report.

In this paper, we propose two novel schemes—iterative per cluster malicious detection (IPCMD) and iterative per cluster malicious detection-accelerated (IPCMD-A)—which can realize secure cooperative spectrum sensing and improve the secondary user's location privacy in the presence of malicious users. These schemes can detect the presence of malicious users without requiring extra resources, and it enables the sensing devices to submit their encrypted sensing data to FC while FC could obtain the sum of all sensing reports without learning each individual values. IPCMD includes a novel self-organized key management scheme, which can support the secondary user dynamic join/leave in cooperative sensing, and it can reduce largely the key management complexity compared to PPSRA.

The contributions of this work are summarized as follows:

1. We propose a novel algorithm for key management based on the relationship between secondary users. This algorithm can work well in a dynamic CR network with untrusted FC. Furthermore, it is resilient against different attacks.
2. We design a novel secure soft combination scheme based on the prioritized sequential probability ratio test, in which the different users are prioritized and regrouped together based on their reputation scores.
3. We confirm the high efficacy and efficiency of our schemes by simulation studies.

The rest of the paper is organized as follows. Section 2 introduces the system and adversary models. Section 3 presents our proposed solution. Section 4 reports the performance evaluation based on detailed simulation studies. Finally, conclusions are drawn in Section 5.

2 System and adversary models

2.1 System model

The adopted system model consists on a centralized cognitive radio (CR) network [16]: a fusion center (FC) and multiple secondary users in a range of 1 to 2 km distributed over n regions (Fig. 1). The set of SUs is denoted

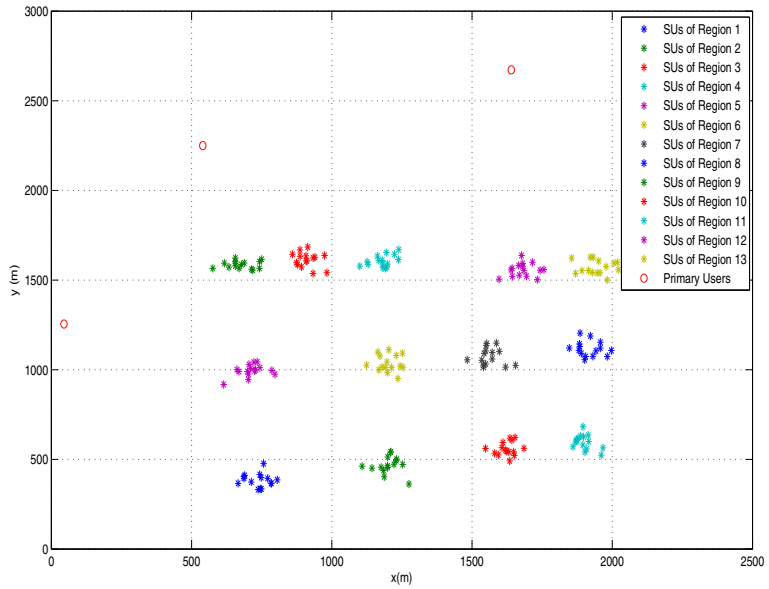

Fig. 1 System architecture

by $U_s = \{U_1, U_2, \ldots, U_n\}$. The considered primary users are mainly TV broadcasts [22], where the transmission power is nearly invariant. We propose to realize secure cooperative spectrum sensing in the presence of malicious mobile detectors. The used spectrum sensing technique is energy detection.

2.2 Spectrum sensing models and signal propagation

We consider the signal propagation model in [23] under which the received primary signal strength at a SU U_i can be expressed as

$$P_i = P_0 \left(\frac{d_0}{d_i}\right)^{\alpha} e^{X_i} e^{Y_i} \tag{1}$$

where d_0 is the reference distance, d_i is the distance from a secondary user U_i to the primary user, P_0 is the received primary signal strength at d_0, α is the path loss exponent with value between 2 and 5, $\exp(X_i)$ and $\exp(Y_i)$ represent, respectively, the effect of shadowing and multi-path fading, and X_i is normally distributed with $\mu = 0$ and variance σ^2: $N(0, \sigma^2)$.

We assume that the channel bandwidth is much larger than the coherent bandwidth, so the effect of multi-path fading is negligible, i.e., $Y_i = 0$ for all U_i [22, 24, 25]. In addition, we assume that X_j and X_i are independent for all $U_i \neq U_j$, i.e., each user experiences i.i.d. Gaussian shadowing and fading, which holds when the distance between U_i and U_j exceeds decorrelation distance [22, 26]. Also, that the nodes are equipped with energy detection which is the most widely used detection technique for its simplicity and efficiency. In fact, during the sensing phase, each node collects m received signal strength RSS samples. The sensing report from user U_i is denoted as $x_i = (x_{i,1}, \ldots, x_{i,m})$. The statistic test of the energy detector is the average RSS (including the noise power) $r_i = \frac{1}{m} \sum_{k=1}^{m} x_{i,k}$.

According to [23] and [27], r_i can be approximated as a Gaussian random variable using the central limit theorem (CLT) as

$$r_i = \begin{cases} \mathcal{N}\left(N_0, 2N_0^2/M\right) & H_0: \text{Primary user is absent} \\ \mathcal{N}\left(N_0 + \bar{P}_i, 2(\bar{P}_i + N_0)^2/M\right) & H_1: \text{Primary user is present.} \end{cases} \tag{2}$$

where $\bar{P}_i = E(P_i)$ is the average received power at user U_i and N_0 is the noise power.

2.3 Adversary model

We assume that the adversary has full control over multiple malicious users who may launch the following attacks:

1. *Privacy threats in collaborative spectrum sensing* [15] Consider an attacker aiming to track the location of secondary users which are involved in cognitive radio networks. This attacker could be a compromised cognitive radio user, an external adversary, or even the untrusted FC. In particular, the single report location privacy (SRLP) attack is considered [15].
2. *Data injection attack* [17, 18, 28] We take into consideration a second type of attack where the malicious users send falsified sensing reports to fool the FC. In fact, a malicious user may:
    - Sends high RSS values during the absence of the primary signal, which increases the probability

of false alarm and prevents CR users from using the channel.
- Sends low RSS values during the presence of the primary signal which increases the probability of miss detection and causes increased interference to the primary user.

Malicious users might be the majority in a region; however, we assume that there are enough secondary users submitting correct sensing reports. Otherwise, it is difficult to realize PU detection with desired false alarm and miss detection probabilities.

3 Location privacy preservation and data injection attack resistance

3.1 Overview

The privacy-preserving aggregation (PPA) scheme [15] allows the identification of the presence or absence of the primary user signal using the sensing reports from different secondary users while preserving their location privacy based on secret key sharing techniques. In fact, the FC shares secret keys among a group of participants so that the FC is able to compute the sum of the participants' keys but not their exact values. Hence, this enables the FC to receive the aggregated sensing reports without learning each individual sensing report value. However, the original PPA scheme is not appropriate for a dynamic CR network because it is limited to the static environment. Hence, the authors in [15] proposed the privacy-preserving sensing report aggregation (PPSRA) protocol to be adaptive and appropriate to the dynamic CR networks where the users may temporarily join/leave. In spite of solving the location privacy issue, PPSRA is not resistant to data injection attack where the malicious users may send falsified reports to the FC. Therefore, in this paper, we enhance the PPA and PPSRA by using special key sharing techniques and special malicious identification protocols which enable IPCMD to work well in a dynamic CR network in the presence of malicious users using data injection attack. In this section, we present the two proposed techniques—IPCMD and IPCMD-A—that allow

- Exploiting the sensing reports of different CR users to obscure the correlation between the report and user location which permits secure spectrum sensing in IPCMD.
- Using prioritized sequential probability ratio test [29], and fine-grained reputation management [30], to enable robust data fusion.

3.2 Iterative per cluster malicious detection

3.2.1 Key generation

We denote by $SK = \{sk_0, sk_1, sk_2, \ldots, sk_n\}$ the secret keys corresponding the secondary users $U_s = \{U_1, U_2, \ldots, U_n\}$ in CR networks and let U_0 be the FC. Let G denote a cyclic group with generator g of prime order p for which decisional Diffie-Hellman is hard and $H : Z \longrightarrow G$ denotes a hash function modeled as a random oracle. To identify the malicious user, we propose in IPCMD to use a special secret key generation technique. In fact, at each time slot, the n secondary users are divided into n_G groups. For example, it is shown in Fig. 2 how 12 SUs are divided randomly into 4 groups of 3 users.

At this step, we differentiate between two different phases:

- *Learning phase*: During the first N_{training} time slots, the groups are selected randomly to increase the probability of making the malicious users participate in the generation of different aggregated reports which allow the system to faster distinguish the attackers.
- *Improvement phase*: After identifying the malicious users during the first N_{training} time slots, the FC selects the groups in a matter to allow better exploitation of the trusted users. In fact, the users are sorted based on their reputation scores (see Section 3.4) and divided into n_G groups so that the best users are grouped together.

Consequently, the keys are generated independently in each group so that the FC can recuperate only the aggregated sensing report of each group and not the exact reports to preserve the location privacy.

For each group g_k from the n_G defined groups, every two nodes u_i, u_j generate randomly their pairwise secret keys $sk_{i,j}$ and $sk_{j,i}$, such that $sk_{i,j} + sk_{j,i} = 0$. The final secret key for a node u_i can be written as

$$sk_i = \sum_{U_j \in g_k} sk_{i,j} \tag{3}$$

Based on Eq. 3, the sum of the secret keys for each group is equal to 0:

$$\sum_{U_i \in g_k} sk_i = \sum_{U_i U_j \in g_k} sk_{i,j} + sk_{j,i} = 0 \tag{4}$$

3.2.2 Encryption

Each secondary user $u_i \in U$ senses the spectrum at the time slot t and then encrypts his sensing report r_i with his secret key as follows:

$$c_i = H(t)^{sk_i} g^{r_i} \tag{5}$$

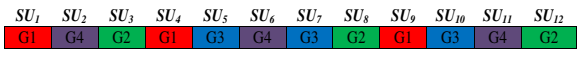

Fig. 2 Group partition in IPCMD

where g is the generator of G and $g^{r_i} = g^{r_i} \bmod p$ and $H(t)^{sk_i} = H(t)^{sk_i} \bmod p$ present two modular exponentiation.

3.2.3 Decryption

After receiving the sensing reports from all CR users, the FC obtains the final aggregated sensing report for each group g_k by first computing

$$R_{g_k} = \prod_{u_i \in g_k} c_i = g^{\sum r_i} H(t)^{\sum Sk_i} \quad (6)$$

The keys are generated so that in each group, $\sum Sk_i = 0$; hence, $H(t)^{\sum Sk_i} = 1$. Consequently, the expression of R_{g_k} becomes

$$R_{g_k} = g^{\sum r_i} \quad (7)$$

Therefore, to obtain the aggregated sensing report for time slot t, the FC needs to compute the discrete log of (R_{g_k} base g) and then obtain $\sum r_i$ which will be used for both the decision (existence or absence of primary user) and in the reputation score determination.

3.3 Prioritized sequential probability ratio test

After receiving the sensing reports from all the users and after sorting the groups based on their reputation scores (see Section 3.4), the FC applies the sequential probability ratio test (SPRT) technique [31]. In fact, the probability ratio V is generated for each group g_k as follows:

$$V = \sum_{U_i \in g_k} \ln \left(\frac{P(r_i|H_1)}{P(r_i|H_0)} \right)^{w_i} \quad (8)$$

where $P(r|H_k)$ presents the probability density function of a random variable r under H_k ($k = 0$ or 1) and $w_i \in [0, 1]$ is the normalized reputation score of user i used as the weight here, which will be explained in Section 3.4.

By using this ratio test, the FC decides whether the primary user is transmitting or not based on the following criterion:

- Accept H_1 and terminate if $V \geq A$;
- Accept H_0 and terminate if $V \leq B$;
- Select another group g_k if $A < V < B$.

Where A and B are the thresholds derived respectively from the desired miss detection probability η and false alarm probability ϕ [22].

According to [23], A and B can be written as follows:

$$A = \ln \left(\frac{1-\eta}{\phi} \right) \quad (9)$$

and

$$B = \ln \left(\frac{\eta}{1-\phi} \right) \quad (10)$$

At each iteration, the FC chooses an aggregated sensing report corresponding to the group g_k with the highest reputation score (see Section 3.4), updates V according to Eq. 12, and checks if a final decision can be reached. In addition, in case where a decision cannot be reached after aggregating all the sensing reports, the FC considers that the primary user is transmitting to avoid interference.

We note that the reputation score generation is most important in the learning phase to distinguish the malicious users. Hence, to reduce the complexity of the algorithm, the reputation score update might be stopped during the improvement phase.

3.4 Fine-grained reputation management

In IPCMD, the reputation scores are used by the FC to differentiate malicious users from normal ones. In fact, the FC records the past sensing performance of each user and it predicts his future performance based on his past long-term behavior. The reputation score generation is built based on [13, 14] which is firmly rooted in the classical Bayesian inference theory used to evaluate one or more unknown quantities from the results of a sequence of multinomial trials. Based on the work in [22], we propose the following algorithm to iteratively assign a reputation score to each user.

First, the algorithm is initialized by defining the different possible intervals I_j of the probability ratio test as follows:

- Let $w = 2(q+1)$ for some integer $q \geq 1$.
- The range $[-\infty, \infty]$ is divided into $2q+2$ intervals, denoted by $(I_1, \ldots, I_{2q+2})$, where A and B ($B \leq 0 \leq A$) are the decision thresholds for the desired miss detection and false alarm probabilities, which correspond to H_1 and H_0.
  The jth interval is given by

$$\begin{cases} (-\infty, B) & \text{If } j = 1 \\ \left(\frac{((k^{q+2-j}-1)B)}{(k^q-1)}, \frac{((k^{q+1-j}-1)B)}{(k^q-1)} \right) & \text{If } 2 \leq j \leq q+1 \\ \left(\frac{((k^{j-q-2}-1)A)}{(k^q-1)}, \frac{((k^{j-q-1}-1)A)}{(k^q-1)} \right) & \text{If } q+2 \leq j \leq 2q+1 \\ (A, \infty) & \text{If } j = 2q+2 \end{cases} \quad (11)$$

  where $k > 1$ is a system parameter. We denote by $|I_j|$ the length of the jth interval. $|I_j|$ can be written as

$$|I_j| = \begin{cases} k\,|I_{j+1}| & \text{If } 2 \leq j \leq q \\ k\,|I_{j-1}| & \text{If } q+2 \leq j \leq 2q \end{cases} \quad (12)$$

  Then, at each time slot, to assign a reputation score for each user, the following algorithm is used.

- After each sensing task, the performance of each group is mapped into one of the w levels based on the determination of $c_i = lnP(r_i|H1) - lnP(r_i|H0)$, [28], which presents the potential contribution of the cluster i (level I_t).
- The performance level of group i is assigned a parameter l_i as follows:

$$l_i = \begin{cases} t & \text{If } H_1 \\ w+1-t & \text{If } H_0 \end{cases} \quad (13)$$

if a group i has a positive (or negative) contribution to the final decision, its sensing performance will be mapped into one of the higher (lower) $q+1$ levels.
- For each $SU_j \in cluster_i$, we have $l_j = l_i$
- We maintain a reputation profile for every SU_j, denoted by $c_{j,s}$ which counts how many times user j got the reputation s.
- If we desire a performance level no less than $l \in [1, \varpi]$, we compute the reputation expectation for each user j as follows:

$$w_j = \sum_{s=1}^{l} c_{j,s} s \quad (14)$$

Our scheme obviously has a good resilience to false sensing reports. In particular, a sensing report from a less reputable user will be given a smaller weight. Hence, it is less likely to affect the final decision. Moreover, a sensing report with low weight will be counted only if a final decision cannot be reached after combining all the other sensing reports with weight. As long as there are sufficient trusted users in a group, a robust decision can still be reached even if there are too many malicious users (seen in Figs. 5 and 6).

3.5 Iterative per cluster malicious detection-accelerated

3.5.1 Key generation

For IPMCD, the bigger the number of groups n_G is, the faster the malicious users can be distinguished and the shorter the learning phase is. In order to reduce the learning phase duration which contains the biggest part of the algorithm complexity, we propose a modified IPMCD which we call IPMCD-A to generate the keys so that the decryption can be done for multiple random groups in only one time slot. Similar to IPCMD, key matrix SK($n * n$) is generated where n is the total number of users. Each user U_i generates the row i in the matrix and sends to user j the needed elementary key $sk_{i,j}$. We describe the key exchange technique using the following Algorithm 1.

Algorithm 1 MGSKI algorithm

procedure $f_{alg}(n, m)$
  for each user U_j **do**
    for each user U_i **do**
      if $i < m$ **then**
        $sk_{i,j} \leftarrow$ random key
      else
        if $i \; mod \; [2] \equiv 0$ **then**
          $sk_{i,j} \leftarrow -\sum_{p=i-m+1}^{i-1}(sk_{p,j})$ (The key is generated such the the sum of the keys in the group $\{U_{i-m+1}, U_{i-m+2}, \ldots, U_i\}$ of size m is equal to zero).
        else
          if $i - m - 1 > 0$ **then**
            $sk_{i,j} \leftarrow -\sum_{p=i-m}^{i-2}(sk_{p,j})$ (The key is generated such the the sum of the keys in the group $\{U_{i-m+2}, U_{i-m+2}, \ldots, U_{i-2}, U_i\}$ of size $m+1$ is equal to zero).
          else
            $sk_{i,j} \leftarrow$ random key
          end if
        end if
      end if
    end for
  end for
  $sk_i \leftarrow \sum_j(sk_{i,j})$ the secret keys are gathered from all the users.
end procedure

After gathering the secret keys from all the users, the final key for user $sk_i = \sum_{j=1}^{n} sk_{i,j}$. Hence, the sum of sk_i can be null in approximately n groups ($n/2$ groups of m users and $n/2$ groups of $m+1$ users) which increases the chances of distinguishing the malicious user faster since they have greater probabilities to participate in the generation of the aggregated sensing report in different groups. For example, it is shown in Fig. 3 how 12 users can be partitioned into 5 groups of 3 users and 4 groups of 4 users. Indeed, the bigger the number of users, the more the number of groups that can be approximated by n.

This algorithm will be executed in each time slot. Hence, compared to IPMCD where each user U_i can appear only

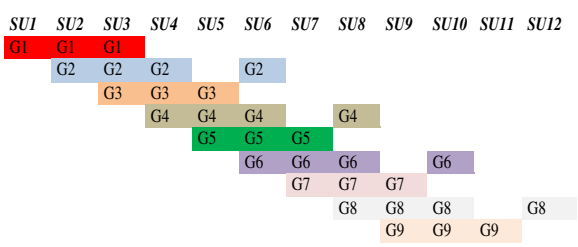

Fig. 3 Group partition in IPCMD-A

in one group per iteration, in IPMCD-A. U_i can be in multiple groups at the same time ($\approx$ 3 times in Fig. 3) which improves the speed of malicious user detection, reduces the learning phase duration, and consequently reduces the complexity of IPMCD.

3.5.2 Encryption and decryption

The same encryption and decryption techniques are used in IPMCD-A compared with IPMCD except that the encrypted sensing report of user U_i is no longer used for the decryption of only one aggregated report but for many ones.

3.5.3 Reputation score management

By updating the reputation score management algorithm of IPMCD, each user in IPMCD-A may update its reputation score multiple times at the same time slot since it participated in the generation of multiple aggregated reports. Hence, less time is needed in the learning phase of IPMCD-A compared to IPMCD.

4 Performance evaluation

In this section, we evaluate the effectiveness and efficiency of the proposed schemes IPCMD and IPCMD-A.

4.1 simulation setup

As in [32], we consider an IEEE 802.22 WRAN environment with a single DTV transmitter with 6-MHz bandwidth and 150.3-km transmission range. We simulate a rectangle cell of 2.5×2.5 km^2. The distance between the center of the cell to the primary user is 145 m. We set the minimum distance between any two detectors to be 200 m to decorrelate their shadow fading X_i [33]. We assume each node is equipped with energy detectors. Note that we used in Fig. 1 only indicative positions for the PUs. In fact, if the primary users are drawn in their real positions (with the correct scale), the figure will not be clear since all the region is 2.5×2.5 km and the primary user distance from its center is 145 km. In addition, we call a malicious user i has an attack strength $T(dB)$ if it reports a $r_i + T$ where r_i is the true average of the RSSI values (the malicious user aims to increase the probability of false alarm by sending high RSS $r_i + T$ values during the absence of the primary signal) [32]. We assume that there are 195 users in total, among which M are malicious.

Table 1 lists the default parameters used in our simulation unless stated otherwise. The simulation is done in MATLAB, and each point is the average of 10,000 runs, each with a random seed.

Table 1 Default simulation setting

Parameter	Value	Description
d_0	1 m	Reference distance
N_0	27 dBm	The noise power
P_0	88 dBm	The received power at d_0
m	6000	Number of samples
α	3.7	Path loss exponent
ϕ	0.01	Desired miss detection probability
η	0.1	Desired false alarm probability
ϖ	22	Total number of performance levels
k	1.4	Ratio between adjacent performance intervals
l	12	Minimum desired performance level

4.2 Simulation results

Figure 4 shows the miss detection probabilities of PPSRA, IPCMD, and IPCMD-A as a function of the number of malicious users. We can see that the miss detection probability of PPSRA system increases with number of malicious users which proves that the PPSRA is non-resistant to the data injection attack in terms of miss detection probability. In addition, it can be seen that the miss detection probability of IPCMD is close to 0 and does not exceed 0.1 when the number of malicious users is below 100 out of 195 users (51.21 % of the users are malicious users). We notice that PPSRA outperforms IPCMD in terms of miss detection probability when the number of malicious users reaches 150 out of 195 (76.91 % of the users are malicious users). In fact, for a large number of malicious users, there is high probability to make a wrong decision from the beginning. Hence, the malicious users will be given bigger reputation scores which will increase the miss detection probability compared with PPSRA system. The miss detection of IPCMD-A is less sensitive to the number of malicious users. In fact, it remains equal to 0 even when the number of malicious users corresponds to 110 from 195 users (56 % of the users are malicious users). In fact, IPCMD-A uses a bigger number of groups in each iteration to distinguish the malicious users which explains why IPCMD-A outperforms IPMCD in terms of miss detection probability.

Figure 5 shows the false alarm probability of PPSRA, IPCMD, and IPMCD-A as a function of the number of malicious users. It can be seen that also in terms of false alarm probability, PPSRA loses its performance when the number of malicious users increases. In addition, the false alarm probability of IPCMD is equal to 0 even for 75 malicious users out of 195 (38 % of the users are malicious users) and it reaches 0.1 for 110 malicious users (56 % of the users are malicious users). Compared to the miss detection probability presented in Fig. 4, the false alarm probability is more sensitive to the number of attackers since in case where the FC cannot be sure if the primary user is using the spectrum or not, it assumes that there is a transmission to prevent possible interferences which may increase the false alarm probability in case of uncertainty.

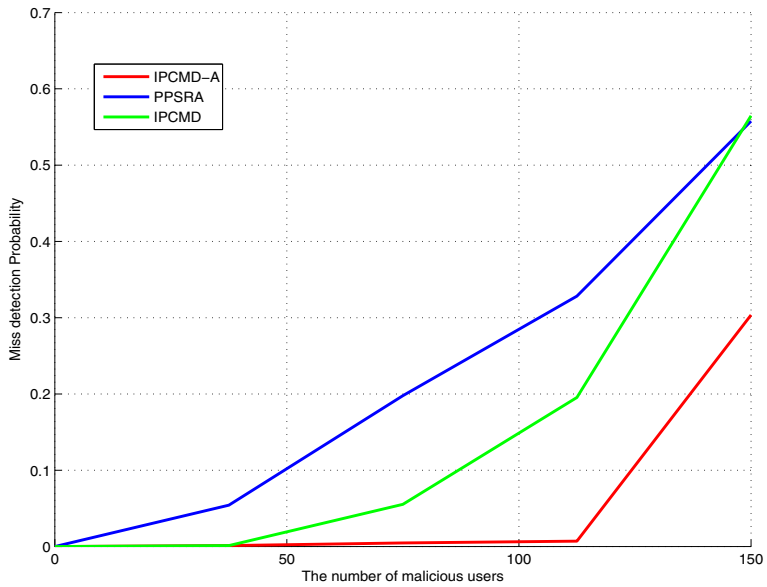

Fig. 4 Miss detection probability vs. number of malicious users

Figure 6 shows the effect of the attack strength on the false alarm probability of PPSRA, IPCMD, and IPMCD-A. The attack strength is varied between 0 and 2×10^{-6} (from 0 to approximately the average power of the received signal if the primary user is really transmitting) and the number of malicious users is fixed to 50 users. We can remark that if the attack strength is bigger than 2×10^{-6} (20 % of the average received power from the primary user if it is really transmitting), false alarm probability for PPSRA starts increasing to reach 0.55 when the attack strength is 0.4×10^{-6}. However, the false alarm probability for IPCMD remains close to 0 when the attack strength is below 1.2×10^{-6} (60 % of the average received power from the primary user if it is really transmitting). On the other hand, it can be seen that IPMCD-A is much resistant and starts getting errors only when the attack strength is equal to 1.8×10^{-6} (90 % of the average received power from the primary user if it is really transmitting). Hence, IPCMD-A outperforms both IPCMD and PPSRA in terms of false alarm probability even when the malicious users send very high RSS values.

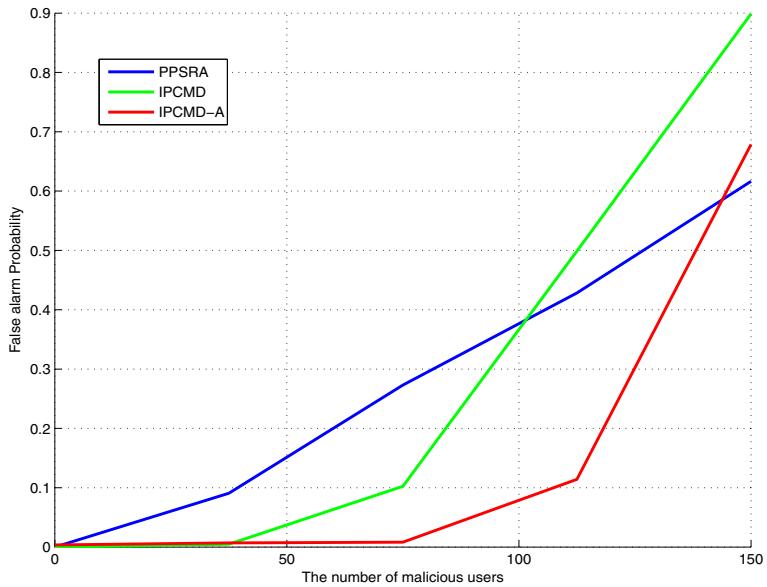

Fig. 5 False alarm probability vs. number of malicious users

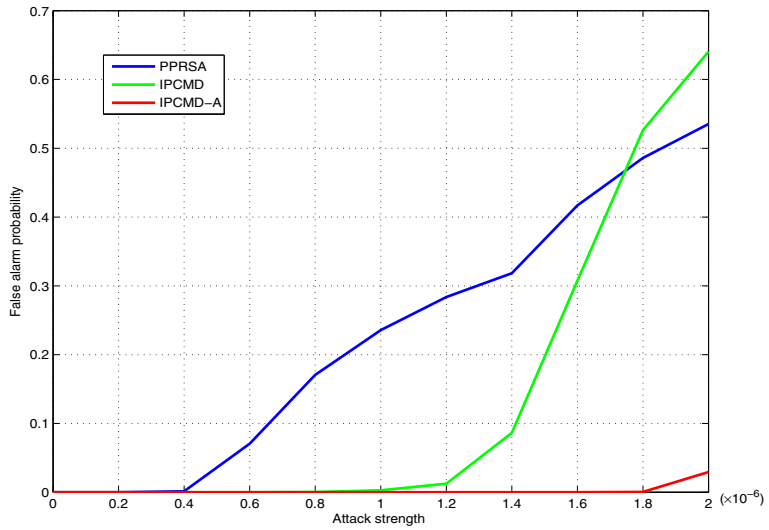

Fig. 6 False alarm probability vs. attack strength

In Fig. 7, since the objective of IPMCD and IPMCD-A is to distinguish the malicious users from the non-malicious ones, we define a new metric which is the reputation sorting error probability. In fact, for all the possible pairs of users malicious and non-malicious, we calculate the probability of giving the malicious users bigger reputation than the normal user. This defined error probability of estimated weight is plotted as a function of the number of iterations where after each 10 iterations, we change the number of malicious users (30, 60, and 90 out of 195). First, that we can remark that during the first 10 iterations (10 malicious users), IPMCD was not able to distinguish the malicious users ($P_W = 0.5$) since they have no sufficient number of groups nor iterations (0.5 for IPMCD and 0.36 for IPMCD-A). We remark also that whatever is the number of malicious users, the difference between IPMCD and IPMCD-A can be seen starting from the first iteration and increases in time. In fact, during the learning phase, the groups are selected randomly to increase the probability of making the malicious users participate in the generation of different aggregated reports which allows the system to distinguish the attackers faster. So, the bigger the number of groups is, the faster the malicious users can be distinguished and the shorter the learning phase is.

Figure 8 presents the reputation score of secondary users after 1 to 100 iterations of the learning phase for IPMCD. It can be seen that the proposed algorithm

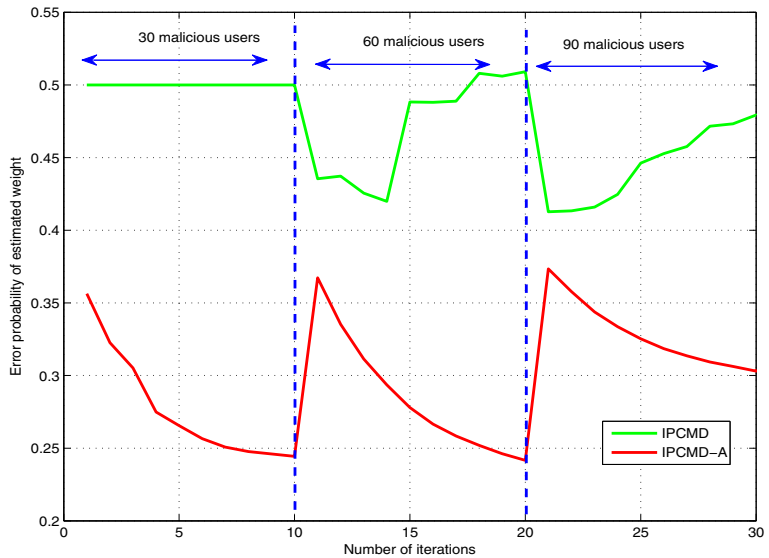

Fig. 7 Error probability of estimated weight vs. number of iterations

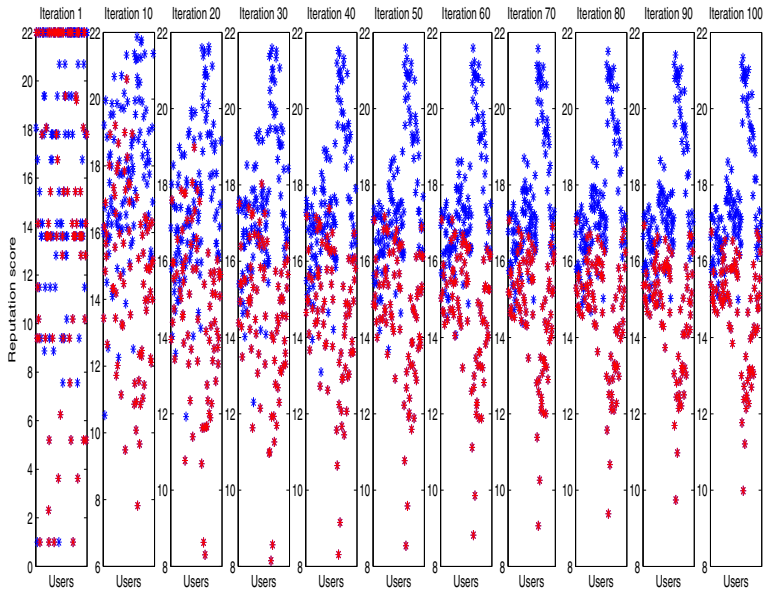

Fig. 8 Reputation score evolution in time

successfully distinguishes the malicious users from the normal SUs by giving them low reputation scores.

4.3 IPCMD Vs IPCMD-A

Figure 6 proves that IPCMD-A is more resistant than IPCMD in data injection attack. The false alarm probability remains less than 0 even when the attack strength is equal to 1.8×10^{-6} while this is not the case for IPCMD. Concerning the localization preservation of secondary users, we can take the example presented in Figs. 2 and 3. We have 12 users divided as 4 groups for IPCMD and 9 groups for IPCMD-A. If the sensing reports keep approximately the same values, after 3 iterations, an attacker can find the extra values of the sensing report for each users in IPCMD, while for IPCMD-A, an attacker needs only to two iterations to find the sensing reports of each users.

In these conditions, we can say that both systems show good results and we have to choose our priority: if we are looking for localization preservation, we have to select IPCMD; and if we are looking for data injection preservation, we have to choose IPCMD-A.

5 Conclusions

In this paper, two novel schemes IPMCD and IPMCDA have been proposed to realize a secure cooperative spectrum sensing. The proposed schemes improve the secondary user's location privacy in the presence of malicious users. These techniques include a novel algorithm for key management which can work well in a dynamic CR network even with untrusted FC. They include also a novel secure soft combination scheme where the different users are prioritized and regrouped together based on their reputation scores. Simulation results showed that both schemes can detect the presence of malicious users while preserving the SU's location. It has been proven also that IPCMD is more efficient in the location preservation and less resistant in data injection attack compared to IPCMD-A.

Competing interests
The authors declare that they have no competing interests.

Acknowledgments
This publication was made possible in part by the sponsorship agreement in support of research and collaboration by Ooredoo, Doha, Qatar. The statements made herein are solely the responsibility of the author[s].

Author details
[1] Department of Electrical Enginnering, Qatar University, Doha, Qatar.
[2] Université de Tunis El Manar, Ecole Nationale d'Ingénieurs de Tunis, LR-99-ES21 Laboratoire de Systèmes de Communications, 1002 Tunis, Tunisia.

Received: 15 May 2015 Accepted: 24 February 2016
Published online: 15 March 2016

References

1. MA McHenry, NSF spectrum occupancy measurements project summary. shared spectrum co. report (2005)
2. H Soy, Z Özdemir, M Bayrak, R Hamila, N Al-Dhahir, Decentralized multiuser diversity with opportunistic packet transmission in MIMO wireless sensor networks. ELSEVIER AEU Int. J. Electron. Commun. **76**(1), 910–925 (2013)
3. S Haykin, Cognitive radio: brain-empowered wireless communications. IEEE J Sel. Areas Commun. **23**(2), 201–220 (2005). doi:10.1109/JSAC.2004.839380
4. IJ Mitola, in *Nationa Telesystems Conference, 1992. NTC-92.I*. Software radios—survey, critical evaluation and future directions, (1992), pp. 13–151323. doi:10.1109/NTC.1992.267870
5. A Bhowmick, SD Roy, S Kundu, in *Twenty First National Conference on Communications (NCC), 2015*. A hybrid cooperative spectrum sensing for cognitive radio networks in presence of fading, (2015), pp. 1–6. doi:10.1109/NCC.2015.7084887

6. EG Larsson, M Skoglund, Cognitive radio in a frequency-planned environment: some basic limits. IEEE Trans. Wirel. Commun. **7**(12), 4800–4806 (2008). doi:10.1109/T-WC.2008.070928
7. A Sahai, N Hoven, R Tandra, in *Proceedings of Allerton Conference on Communications, Control and Computing*. Some fundamental limits in cognitive radio, (2004)
8. AE Shafie, N Al-Dhahir, R Hamila, in *2015 IEEE Wireless Communications and Networking Conference, WCNC 2015, New Orleans, LA, USA, March 9–12, 2015*. Exploiting sparsity of relay-assisted cognitive radio networks, (2015), pp. 1153–1158. doi:10.1109/WCNC.2015.7127632. http://dx.doi.org/10.1109/WCNC.2015.7127632
9. AC Sumathi, R Vidhyapriya, in *International Conference on Intelligent Systems Design and Applications (ISDA), 2012 12th*. Security in cognitive radio networks—a survey, (2012), pp. 114–118. doi:10.1109/ISDA.2012.6416522
10. R Saeed, in *Mosharaka International Conference on Communications, Computers and Applications, 2008. MIC-CCA 2008*. Cognitive radio and advanced spectrum management, (2008). doi:10.1109/MICCCA.2008.4669836
11. A Celik, R Saifan, AE Kamal, in *International Conference on Computing, Networking and Communications (ICNC), 2015*. Sensing strategies for channel discovery in cognitive radio networks, (2015), pp. 637–641. doi:10.1109/ICCNC.2015.7069419
12. M Cardenas-Juarez, U Pineda-Rico, E Stevens-Navarro, M Ghogho, in *International Conference on Electronics, Communications and Computers (CONIELECOMP), 2015*. Sensing-throughput optimization for cognitive radio networks under outage constraints and hard decision fusion, (2015), pp. 80–86. doi:10.1109/CONIELECOMP.2015.7086929
13. AG Fragkiadakis, EZ Tragos, IG Askoxylakis, A survey on security threats and detection techniques in cognitive radio networks. IEEE Commun. Surv. Tutor. **15**(1), 428–445 (2013). doi:10.1109/SURV.2011.122211.00162
14. KK Chauhan, AKS Sanger, in *International Conference on Electronics and Communication Systems (ICECS), 2014*. Survey of security threats and attacks in cognitive radio networks, (2014), pp. 1–5. doi:10.1109/ECS.2014.6892537
15. S Li, H Zhu, Z Gao, X Guan, K Xing, X Shen, in *IEEE Proceedings INFOCOM, 2012*. Location privacy preservation in collaborative spectrum sensing, (2012), pp. 729–737. doi:10.1109/INFCOM.2012.6195818
16. O Fatemieh, A Farhadi, R Chandra, C Gunter, in *18th Annual Network & Distributed System Security Symposium (NDSS)*. Using classification to protect the integrity of spectrum measurements in white space networks (Internet Society, 2011). http://research.microsoft.com/apps/pubs/default.aspx?id=141605
17. S Althunibat, V Sucasas, H Marques, J Rodriguez, R Tafazolli, F Granelli, On the trade-off between security and energy efficiency in cooperative spectrum sensing for cognitive radio. IEEE Commun. Lett. **17**(8), 1564–1567 (2013). doi:10.1109/LCOMM.2013.062113.130759
18. H Li, X Cheng, K Li, C Hu, N Zhang, W Xue, Robust collaborative spectrum sensing schemes for cognitive radio networks. IEEE Trans. Parallel Distrib. Syst. **25**(8), 2190–2200 (2014). doi:10.1109/TPDS.2013.73
19. S Althunibat, BJ Denise, F Granelli, in *Globecom Workshops (GC Wkshps), 2014*. Secure cluster-based cooperative spectrum sensing against malicious attackers, (2014), pp. 1284–1289. doi:10.1109/GLOCOMW.2014.7063610
20. W Wang, L Chen, KG Shin, L Duan, in *INFOCOM, 2014 Proceedings IEEE*. Secure cooperative spectrum sensing and access against intelligent malicious behaviors, (2014), pp. 1267–1275. doi:10.1109/INFOCOM.2014.6848059
21. L Khalid, A Anpalagan, in *Personal Indoor and Mobile Radio Communications (PIMRC), 2011 IEEE 22nd International Symposium On*. A weighted fusion scheme for cooperative spectrum sensing based on past decisions, (2011), pp. 354–358. doi:10.1109/PIMRC.2011.6139981
22. R Zhang, J Zhang, Y Zhang, C Zhang, in *IEEE Proceedings INFOCOM, 2013*. Secure crowdsourcing-based cooperative spectrum sensing, (2013), pp. 2526–2534. doi:10.1109/INFCOM.2013.6567059
23. SJ Shellhammer, SSND Tandra, J Tomcik, Performance of power detector sensors of DTV signals in IEEE 802.22 WRANs. 2000 5th Int. Symp. Antennas Propag. EM Theory. ISAPE 2000 (IEEE Cat. No.00EX417) (2006). doi:10.1145/1234388.1234392
24. K Siwiak, *Radiowave Propagation and Antennas for Personal Communications, Second Edition*, 2nd edn. (Artech House, Inc., Norwood, 1998)
25. TS Rappaport, *Wireless communications: principles and practice, second edition*, 2nd edn. (Pearson Education, Singapore, 2002)
26. A Algans, KI Pedersen, PE Mogensen, Experimental analysis of the joint statistical properties of azimuth spread, delay spread, and shadow fading. IEEE J. Sel. Areas Commun. **20**(3), 523–531 (2002). doi:10.1109/49.995511
27. R Tandra, A Sahai, SNR walls for signal detection. IEEE J. Sel. Top. Sign. Process. **2**(1), 4–17 (2008). doi:10.1109/JSTSP.2007.914879
28. F Penna, Y Sun, L Dolecek, D Cabric, in *IEEE Global Telecommunications Conference (GLOBECOM 2011), 2011*. Joint spectrum sensing and detection of malicious nodes via belief propagation, (2011), pp. 1–5. doi:10.1109/GLOCOM.2011.6133986
29. F Hu, S Wang, Z Cheng, in *IEEE Military Communications Conference, 2009. MILCOM 2009*. Secure cooperative spectrum sensing for cognitive radio networks, (2009), pp. 1–7. doi:10.1109/MILCOM.2009.5379961
30. M Zhou, J Shen, H Chen, L Xie, in *IEEE Wireless Communications and Networking Conference (WCNC), 2013*. A cooperative spectrum sensing scheme based on the Bayesian reputation model in cognitive radio networks, (2013), pp. 614–619. doi:10.1109/WCNC.2013.6554634
31. R Chen, J-M Park, K Bian, in *The 27th Conference on Computer Communications. IEEE INFOCOM 2008*. Robust distributed spectrum sensing in cognitive radio networks, (2008). doi:10.1109/INFOCOM.2008.251
32. AW Min, KG Shin, X Hu, in *17th IEEE International Conference on Network Protocols, 2009. ICNP 2009*. Attack-tolerant distributed sensing for dynamic spectrum access networks, (2009), pp. 294–303. doi:10.1109/ICNP.2009.5339675
33. A Algans, KI Pedersen, PE Mogensen, Experimental analysis of the joint statistical properties of azimuth spread, delay spread, and shadow fading. IEEE J. Sel. Areas Commun. **20**(3), 523–531 (2002). doi:10.1109/49.995511